楕円曲線の局所ルートナンバーについて (代数的整数論とその周辺)

AUTHOR(S):

小林, 真一

CITATION:

小林, 真一. 楕円曲線の局所ルートナンバーについて (代数的整数論とその周辺). 数理解析研究所講究録 2000, 1154: 55-65

ISSUE DATE:

2000-05

URL:

http://hdl.handle.net/2433/64129

数理解析研究所講究録
1154巻 2000年 55-65

楕円曲線の局所ルートナンバーについて

小林 真一
KOBAYASHI SHINICHI

目次

1. Introduction

今回の話の目的は楕円曲線に付随する L-関数の関数等式の符号を記述することである。この符号はMordell-Weil群の階数の偶奇になると予想され、このような重要な不変量を簡単に計算できるところが興味深い点である。もちろんHasse-Weil予想が証明されていない現在、関数等式の符号というものに意味あるのか?、その計算とは?という疑問がわく。その点を明らかにするためにも、もう少し詳しく話をしよう。

F を代数体、E を F 上の楕円曲線とする。このとき E/F の L-関数が次のように定義される:

$$L(E/F,s) := \prod_{\text{よい素点}} \frac{1}{1-a_v q^{-s}+q^{-2s+1}} \times \prod_{\text{乗法的悪点}} \frac{1}{1\pm q^{-s}} .$$

ここで $a_v := 1-\sharp E(k_v)+q$、$\sharp E(k_v)$ はreductionして得られる楕円曲線の k_v 有理点の個数である。Hasse-Weil予想によれば $L(E/F,s)$ は全複素平面に解析接続され、$L(E/F,s)$ に Γ 因子をかけて得られる $\Lambda(E/F,s)$ は、関数等式

$$\Lambda(E/F,s) = w\Lambda(E/F,2-s)$$

を満たす。ここで $w=\pm 1$ が関数等式の符号である。定義からただちに $w=(-1)^{\mathrm{ord}_{s=1}L(E/F,s)}$ であるが、Birch-Swinnerton-Dyer予想を認めると $w=(-1)^{\mathrm{rank}E(F)}$ と書ける。

さて今までは w の定義を含めて様々な予想に立脚していたが、Langlandsはこれらの予想とは独立に w となるべき符号を定義した。実際、$\mathbb{Q}$ 上の楕円曲線に対してはHasse-Weil予想は正しく、関数等式の符号 w が定義されるが、彼の定義した符号はこの w と一致する。

彼はまず局所的に符号 $w(E/F_v)$ を定義し、大域的な符号 $w(E/F)$ はそれらの積として定義する:

$$w(E/F) = \prod_{\text{all places } v} w(E/F_v).$$

局所ルートナンバー $w(E/F_v)$ の定義は複雑なので、次のセクションに任せることにしよう。

今回の主結果は，局所ルートナンバー を Weierstraß 方程式の係数によって記述するものである。potentially multiplicativeな楕円曲線や $F_v=\mathbb{Q}_p$ で $p\geq 5$ のときはRohrlich [8] によってそのような公式が得られていた。今回は剰余体の標数が2でな

東京大学数理科学研究科 博士課程 2年, e-mail koba@ms406ss5.ms.u-tokyo.ac.jp.

い任意の局所体に対し公式を与える。公式は E の Néron model のタイプによって場合分けされる。

Theorem 1.1. K を局所体、剰余体 k の標数は 2 でないとする。E を K 上の楕円曲線で、*Weierstraß* 方程式 $y^2 = x^3 + ax^2 + bx + c$ で与えられるものとする。Δ で上の 3 次式の判別式、$\left(\frac{}{k}\right)$ で k の平方剰余記号を表わす。このとき

i) もし E がタイプ I または $I_0{}^*$ ならば、

$$w(E/K) = \left(\frac{-1}{k}\right)^{\frac{v(\Delta)}{2}}.$$

ii) もし E がタイプ III または III^* ならば、

$$w(E/K) = \left(\frac{-2}{k}\right).$$

iii) E がタイプ II, IV, IV^* または II^* とする。このとき $3 \nmid v_K(c)$ かつ $p \nmid v_K(c)$ なる *Weierstraß* 方程式が存在し、

$$w(E/K) = \delta\,(\Delta\,, v_K(c)c)_v \left(\frac{-1}{k}\right)^{\frac{v(\Delta)(v(\Delta)-1)}{2}}.$$

ここで δ は $\Delta^{\frac{1}{2}} \in K$ ならば 1、そうでなければ -1 とする。$(\ ,\ )_v$ は K のヒルベルト記号である。

Remark 1.1. $p \geq 5$ 以上の場合は定理の *iii)* の δ は $\left(\frac{-3}{k}\right)$ である。これから $w(E/K)$ は $v_K(\Delta)$ が mod 4 で 0、2 に応じて $\left(\frac{-3}{k}\right)$、$\left(\frac{-1}{k}\right)$ となる。これは Rohrlich [8] の公式と一致する。

2. 局所ルートナンバーの定義

局所ルートナンバーの定義を簡単に思い出しそう。詳しくは Deligne [1] や Rohrlich [7] を見ていただきたい。

K を局所体、k をその剰余体とする。W_K で K の Weil 群を表わす。これは $\mathrm{Gal}(\overline{K}/K)$ の部分群で、惰性群と $\mathrm{Gal}(\overline{k}/k)$ のフロベニウスの持ち上げによって生成されるものである。

局所ルートナンバーは ϵ-因子というものの符号として定義されるが、それは楕円曲線に限らず, 任意の Weil(-Deligne) 群の連続表現に対して定義される。定義は Brauer の定理を使って 1 次元の場合に帰着してなされるので、まずその場合から始めよう。

Definition 1. L を K の有限次拡大体とする。χ を 指標（*quasi-character* ）$\chi : L^\times \to \mathbb{C}^\times$ とし、局所類体論によって W_L の指標と見なすことにする。ただし相互写像は数論的フロベニウスを素元に対応させるものとする。ψ を加法的指標 $\psi : L \to \mathbb{C}^\times$、$dx$ を L の *Haar* 測度とする。

このとき χ, ψ, dx に付随する ϵ-因子は以下のように定義される。

$$\epsilon(\chi, \psi, dx) = \begin{cases} \int_{h^{-1}O_L{}^\times} \chi^{-1}(x)\psi(x)\,dx, & \chi \text{ が分岐} \\ \chi(h)\|h\|_L^{-1} \int_{O_L{}^\times} dx, & \chi \text{ が不分岐} \end{cases}$$

ここで $n(\psi)$ は $\psi(\pi^{-n}O_L) = 1$ となる最大の n、$a(\chi)$ は χ の導手、つまり $\chi(U_L^n) = 1$ となる最小の n。h は $L^\times$ の元で 付値が $n(\psi) + a(\chi)$ のもの。$\|\ \|_L$ は L の正規付値である。

局所ルートナンバー $w(\chi,\psi)$ は次のように定義される。

$$w(\chi,\psi) := \frac{\epsilon(\chi,\psi,dx)}{|\epsilon(\chi,\psi,dx)|}.$$

分母は複素絶対値で dx に依らないことはすぐにわかる。

さて楕円曲線の局所ルートナンバーを定義しよう。k の標数と異なる素数 l に対し、Tate module $V_l(E) = T_l(E) \otimes \mathbb{Q}_l$ への自然なガロワ表現を考える。適当な埋め込み $\mathbb{Q}_l \hookrightarrow \mathbb{C}$ を固定しこれを $\mathbb{C}$ 上の表現と見なす。さらにこれを W_K に制限したものを σ_E とおく：

$$\sigma_E : W_K \longrightarrow \mathrm{GL}_2(V_l(E) \otimes_{\mathbb{Q}_l} \mathbb{C}).$$

この σ_E に対し局所ルートナンバーを定義する。今剰余体の標数 p が 2 でないとすると、σ_E は指標の直和になるか、K のある 2 次拡大からくる指標の誘導表現になる。

Definition 2. $p \neq 2$、E は *potential good reduction* をもつとする。
i) $\sigma_E = \chi \oplus \chi'$ ならば、

$$w(E/K) := w(\chi,\psi)w(\chi',\psi).$$

ii) $\sigma_E = \mathrm{ind}_{H/K}\chi$ ならば、

$$w(E/K) := w(\eta,\psi)w(\chi,\psi_H),$$

ここで η は指標 $K^\times \to K^\times/N_{H/K}H^\times \cong \pm 1 \in \mathbb{C}$ である。また ψ は K の任意の加法的指標で $\psi_H = \psi \circ \mathrm{Tr}_{H/K}$ である。

上の定義は χ や ψ の取り方などによらない (c.f. Deligne [1])。

Remark 2.1. $p = 2$ のときも Brauer の定理を使って同様に定義される。E が potential multiplicative reduction をもつときは、σ_E の作り方がもっと複雑になる (例えば Rohrlich [7])。

3. 局所ルートナンバー公式の証明

公式の証明は σ_E が tame か wild かによって複雑さがまったく異なる。p が 5 以上であったり、公式の i)、ii) の場合が tame である。Rohrlich が行ったのは tame の場合であり、彼の方法は一般の局所体に対しても素直に一般化できる。しかし wild、とくに σ_E の導手が奇数の場合はまったく異なる手法を必要とし、σ_E に関するかなり精密な解析が必要になる。ここでは細部に立ち入らず、tame の場合と wild の場合の証明のアイデアを紹介したい。

まずは σ_E の構造を調べるところから始める。σ_E がどのような条件下で指標の直和になるのか調べるのが目標である。

E は potential good reduction を持つので、惰性群の σ_E による像は有限であるが、まずはその構造から。

Theorem 3.1 (Kraus [5]). $p \geq 3$、Λ を σ_E による惰性群の像とする。K^{un} 上で E が *good reduction* をもつ最小の体 L は $K^{un}(E[2], \Delta^{\frac{1}{4}})$ であり、特に Λ は $\mathrm{Gal}(L/K^{un})$ に同型である。これから Λ の構造は

i) $\Lambda \cong \{1\} \Leftrightarrow E$ はタイプ I。
ii) $\Lambda \cong \mathbb{Z}/2\mathbb{Z} \Leftrightarrow E$ はタイプ I_0^*。
iii) $\Lambda \cong \mathbb{Z}/4\mathbb{Z} \Leftrightarrow E$ はタイプ III または III^*。
iv) $\Lambda \cong \mathbb{Z}/3\mathbb{Z} \Leftrightarrow v_K(\Delta) \equiv 0 \mod 4$ で E はタイプ I でない。
v) $\Lambda \cong \mathbb{Z}/6\mathbb{Z} \Leftrightarrow v_K(\Delta) \equiv 2 \mod 4$ で E でタイプ I_0^* でない。

vi) $\Lambda \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} \Leftrightarrow v_K(\Delta) \equiv 1 \mod 2$ で E はタイプ III または III^* でない。

Proof. よく知られているように、L は $m \geq 3$、$p \nmid m$ に対し $L = K^{un}(E[m])$ と書ける。これより $L \supseteq K^{un}(E[2])$、また $v_L(\Delta) \equiv 0 \mod 12$ より $\Delta^{\frac{1}{4}} \in L$。もう少し頑張ると $L = K^{un}(E[2], \Delta^{\frac{1}{4}})$ が出る (c.f. Kraus [5])。また後から実際に $K(E[2], \Delta^{\frac{1}{4}})$ 上で smooth モデルを見つけるのでそれからもわかる。Λ の構造は 2 分点の状況とタイプの関係をみればわかる。例えば、K^{un} に 2 分点が全て入っていれば、E はタイプ I または I_0^*、1 つだけ入っていればタイプ III または III_0^* 等。 □

次に $\mathrm{Im}\,\sigma_E$ がアーベル群になる条件を求める。σ_E は半単純 2 次元複素表現なので (例えば Rohrich [7])、σ_E が可約であることと、$\mathrm{Im}\,\sigma_E$ がアーベルであることは同値である。

Proposition 3.2. *i)* E がタイプ I または I_0^* ならば、$\mathrm{Im}\,\sigma_E$ はアーベル。
ii) E がタイプ III または III^* ならば、$\mathrm{Im}\,\sigma_E$ がアーベル $\Leftrightarrow \left(\frac{-1}{k}\right) = 1$.
iii) E がタイプ II, IV, IV^* または II^* ならば、$\mathrm{Im}\,\sigma_E$ がアーベル $\Leftrightarrow \Delta^{\frac{1}{2}} \in K$.

Proof. iii) の場合だけ示す。他の場合も同様である。Theorem 3.1 より $v_K(\Delta)$ は偶数としてよい。もし $\Delta^{\frac{1}{2}}$ が K の元ならば、$\mathrm{Gal}(K(E[2], \Delta^{\frac{1}{4}})/K)$ は位数 3 または 6 の巡回群である。これより $\mathrm{Gal}(L/K)$、従ってその部分群 $\mathrm{Im}\,\sigma_E$ はアーベルである。$\Delta^{\frac{1}{2}} \notin K$ としよう。Theorem 3.1 より $\mathrm{Im}\,\sigma_E$ の商で $\mathrm{Gal}(K(E[2])/K)$ と同型なものがある。しかし仮定によりこれは 3 次の対称群に同型なのでアーベルではない。 □

Corollary 3.3. *i)* $\mathrm{Im}\,\sigma_E$ がアーベルならば

$$\sigma_E = \chi \oplus \chi^{-1} \| \ \|_K,$$

ここで χ は $K^\times$ のある指標である。
ii) $\mathrm{Im}\,\sigma_E$ が非可換ならば

$$\sigma_E = \mathrm{ind}_{W_H}^{W_K} \chi = \mathrm{ind}_{H/K} \chi,$$

ここで H は *Proposition 3.2* の *ii)*、*iii)* に応じて、$K(\sqrt{-1})$、$K(\Delta^{\frac{1}{2}})$ である。また χ はある $H^\times$ の指標である。

Proof. i) は $\det \sigma_E = \| \ \|_K$ からただちにわかる。ii) は Proposition 3.2 により σ_E の W_H への制限はアーベルな像をもつことから、簡単な群論的考察でわかる。 □

さて公式の証明に入ろう。まず一般的に ϵ-因子がどのような形をしているか述べよう。Henniart [3] によれば、Weil 群の表現 σ に付随する ϵ-因子は、σ から定まるある指標 χ と、付値が σ の swan 導手であるようなある元 ξ を使って、

$$\epsilon(\sigma, \psi, dx) = \chi(\xi) \times \text{ある種のガウス和} \times 1 \text{の} p \text{巾根}$$

と書ける。ここでガウス和は ψ, ξ のみによる。Henniart の結果は wild homogeneous と呼ばれる表現に限っているが、ϵ-因子の形を本質的に物語るものである。楕円曲線からくる表現に関しても、基本的にはこの形をしており、ξ を決定し $\chi(\xi)$ とガウス和からくる符号を求めるのが問題となる。後の応用とこの辺りの事情を理解してもらうために、まずは指標に付随する ϵ-因子に関して Henniart の公式にあたるものを見よう。

$a, b \in \mathbb{C}^\times$ に対し、ab^{-1} が正の実数であるとき $a \sim b$ と書くことにする。

Proposition 3.4. $p \neq 2$ で χ、ψ、dx は *Definition 1* と同じとする。ただし ψ は $n(\psi) = -1$ を満たすようにとる。
i) 導手 $a(\chi)$ が 1 のとき、

$$\epsilon(\chi, \psi, dx) \sim \sum_{x \in k_L} \left(\frac{x}{k_L}\right) \psi(x).$$

ii) 導手 $a(\chi)$ が 1 以外の奇数のとき、

$$\epsilon(\chi, \psi, dx) \sim \chi(\xi^{-1}) \times \sum_{x \in k_L} \left(\frac{x}{k_L}\right) \psi(vx/2) \times \psi(\xi),$$

ここで ξ は L の元で、付値が $a(\chi) - 1/2$ 以上の全ての x に対し、$\chi(1 + x + \frac{x^2}{2}) = \psi(\xi x)$ を満たすもの。また $v = \xi \pi_L^{-v_L(\xi)}$、ここで π_L は L の素元である。
iii) 導手 $a(\chi)$ が偶数のとき、

$$\epsilon(\chi, \psi, dx) \sim \chi(\xi^{-1}) \times \psi(\xi),$$

ここで ξ は L の元で、付値が $a(\chi)/2$ 以上の全ての x に対し、$\chi(1 + x) = \psi(\xi x)$ を満たすものとする。

Proof. これは簡単な積分の計算である。例として iii) の場合を計算してみよう。

$$\begin{aligned}
\epsilon(\chi, \psi, dx) &= \int_{\xi {O_L}^\times} \chi^{-1}(x)\psi(x)\, dx \\
&= \sum_{u \in R} \int_{U_L^{a(\chi)/2}} \chi^{-1}(\xi u x)\psi(\xi u x)\|\xi\|_L\, dx \\
&= \sum_{u \in R} \chi^{-1}(\xi u)\psi(\xi u) \int_{\pi_L^{a(\chi)/2} O_L} \chi^{-1}(1 + y)\psi(\xi u y)\|\xi\|_L\, dy \\
&= \sum_{u \in R} \chi^{-1}(\xi u)\psi(\xi u) \int_{\pi_L^{a(\chi)/2} O_L} \psi(\xi y(1 - u))\|\xi\|_L\, dy \\
&= \chi^{-1}(\xi)\psi(\xi)\|\xi\|_L \int_{\pi_L^{a(\chi)/2} O_L} dy
\end{aligned}$$

1 行目は定義と関係式 $\chi(1 + x) = \psi_L(\xi x)$ から $v_L(\xi) = -a(\chi) + 1$ がわかるため。2 行目は変数変換 $x \leftrightarrow \xi x$ と $R = O_L^\times / U_L^{a(\chi)/2}$ への coset 分解。3 行目は変数変換 $x \leftrightarrow 1 + y$ で、4 行目は関係式 $\chi(1 + x) = \psi_L(\xi x)$ から。5 行目は $u \equiv 1 \mod \pi_L^{a(\chi)/2} O_L$ でなければ、加法的写像 $y \mapsto \psi(\xi y(1 - u))$ が non-trivial になり、積分すると 0 になるため。 □

これから σ_E に付随する ϵ-因子に対して Henniart の公式にあたるものをみよう。σ_E が可約または tame のときは、ガウス和が偶数巾（零巾も含む）になって現れるため、ガウス和の符号を決定する微妙な問題は生じない。そのため Rohrlich による Fröhlich-Queyrut の定理を使った簡単な計算方法が存在する。

Proposition 3.5. σ_E は可約または *tame* とし、χ は $\sigma_E = \chi \oplus \chi^{-1}\| \ \|_K$ または $\sigma_E = \mathrm{ind}_{H/K}\chi$ を満たすものとする。このとき

$$w(E/K) \sim \chi(\xi) \times \pm 1,$$

ここで ξ は σ_E が可約ならば -1、E がタイプ III または III^* ならば $\sqrt{-1}$、E がタイプ II, IV, IV^* または II^* ならば $\Delta^{\frac{1}{2}}$ である。また ± 1 は σ_E が可約ならば 1、そうでなければ -1。

Proof. σ_E が可約のときは、簡単な積分の計算（フーリエ変換）により $w(E/K) = w(\chi,\psi)w(\chi^{-1}\| \ \|_K,\psi) = \chi(-1)$ がわかる（詳しくは Tate [11] を参照)。以下 $\sigma_E = \mathrm{ind}_{H/K}\chi$ としよう。まず誘導表現の determinant に関する公式 (c.f. Deligne [1], Proposition 1.2) から $\chi\,|_{K^\times} = \eta\cdot\| \ \|_K$ がわかる。ここで tame という条件から H/K が不分岐であるので (Corollary 3.3 + Ogg's formula)、$H^\times$ の不分岐指標 κ で $\chi\kappa\,|_{K^\times}$ を trivial にするものがある。これより Fröhlich-Queyrut の定理を使えば $w(\chi\kappa,\psi_H) = \chi(\xi)$ がわかる。一方 κ が不分岐だから $w(\chi\kappa,\psi_H) = w(\chi,\psi_H)(-1)^{n(\psi_H)+a(\chi)}$。やはり H/K が不分岐であることから $w(\eta,\psi) = (-1)^{n(\psi)}$。以上から $w(E/K) = w(\eta,\psi)w(\chi,\psi_H) = -\chi(\xi)$。 □

この場合 $w(E/K)$ は上の命題からただちに決定されるが、紙面の都合上省略させていただく。例えば σ_E が可約で、E がタイプ III または III^* ならば、$\chi|_{O_K^\times}$ の位数は Λ の位数 4 であり、$w(E/K) = \chi(-1) = \chi(\sqrt{-1})^2 = \left(\frac{\sqrt{-1}}{k}\right) = \left(\frac{-2}{k}\right)$ といった具合である。

次に wild で既約な σ_E に対して Henniart の公式にあたるものをみよう。wild であることは、$p=3$ で E がタイプ II, IV, IV^* または II^* と同値であることに注意しておく。まずは記号を定めよう。

M, H をそれぞれ $K(E[2]), K(\Delta^{\frac{1}{2}})$ とする。この場合 M/H は 3 次の完全分岐拡大である。次に同型 $\phi : \mathrm{Gal}(M/H) \to \mathbb{F}_3$ を固定し、$\phi(1)^{-1}$ を g_ϕ と書くことにする。また g_ϕ を W_H の元に K^{un} と $\Delta^{\frac{1}{4}}$ を固定するように延長しておく。さらに E の 2 分点の x-座標 α, β, γ を $g_\phi(\alpha) = \beta$ となるように取り、$\Delta^{\frac{1}{2}}$ を $(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$ として固定し $\Delta^{\frac{1}{4}}$ をその平方根とする。

Proposition 3.6. σ_E は既約かつ *wild* とする。$\sigma_E = \mathrm{ind}_{H/K}\chi$ と書くと、$\chi(g_\phi)$ は 1 の原始 3 乗根で、

$$w(E/K) \sim \chi(\delta_\phi) \times \left(\frac{-1}{k}\right) G_H \times 1 \text{の} 3 \text{巾根}.$$

ここで $\delta_\phi = N_{M/H}(1 - g_\phi\pi_M/\pi_M)$、$G_H$ はガウス和 $\sum_{u\in k_H^\times}\left(\frac{u}{k_H}\right)\chi(g_\phi)^{\mathrm{Tr}_{k_H/\mathbb{F}_3}(u)}$ である。

Proof. ここでは細部には立ちいらず、アイデアだけ紹介する。まず定義により $w(E/K) = w(\chi,\psi_H)w(\eta,\psi)$ である。ψ を $n(\psi_H) = -1$ で、ψ_H の O_H への制限が $O_H \to \mathbb{C}^\times, x \mapsto \chi(g_\phi)^{\mathrm{Tr}_{k_H/\mathbb{F}_3}(\overline{x})}$ となるように取る。この ψ に対し $w(\chi,\psi_H)$、$w(\eta,\psi)$ を Proposition 3.4 を使って計算する。$w(\eta,\psi)$ の方は $a(\chi)$ が奇数ならば -1、$a(\chi)$ が偶数ならば $\left(\frac{-1}{k}\right)G_H$ であることがただちにわかる。non-trivial なのは $w(\chi,\psi_H)$ の計算において、$\chi(\xi)$ が 1 の 3 巾根を除き $\chi(\delta_\phi)$ に等しいことを示すことである。これをみるには $u = \xi\delta_\phi$ が modulo π_H で 1 に合同であることをみればよい。アイデアは任意の $v \in O_H$ に対し、$\chi(1+\delta_\phi v)$ を 2 通りの仕方で計算することである。まず定義により $\chi(1+\delta_\phi v) = \psi_H(uv) = \chi(g_\phi)^{\mathrm{Tr}_{k_H/\mathbb{F}_3}(\overline{uv})}$。他方、Serre [9], Chapter 4 XV,§3, exercise 1 により、局所類体論の相互写像を具体的に記述する次のダイアグラムが

ある。

$$\begin{array}{ccc} {U_H}^t/{U_H}^{t+1} & \xrightarrow{r} & \mathrm{Gal}(M/H) \\ {\scriptstyle \phi_H}\downarrow & & {\scriptstyle \phi}\downarrow \\ k_H & \xrightarrow{\mathrm{Tr}_{k_H/\mathbb{F}_3}} & \mathbb{F}_3, \end{array}$$

ここで $t = a(M/H) - 1$、r は局所類体論の相互写像、ϕ_H は同型 $x \mapsto (x-1)/\delta_\phi$。このダイヤグラムにより $\chi(1+\delta_\phi v) = \chi(g_\phi)^{\mathrm{Tr}_{k_H/\mathbb{F}_3}(\overline{v})}$ を得る。任意の $v \in O_H$ に対し $\chi(g_\phi)^{\mathrm{Tr}_{k_H/\mathbb{F}_3}(\overline{uv})} = \chi(g_\phi)^{\mathrm{Tr}_{k_H/\mathbb{F}_3}(\overline{v})}$ がわかったので、u は modulo π_H で 1 である。 □

次に δ_ϕ を Weierstraß 方程式の係数を使って表わそう。

Proposition 3.7. $p \geq 3$、E のタイプは II, IV, IV^* または II^* とする。このとき *Weierstraß* 方程式 $y^2 = x^3 + ax^2 + bx + c$ で $3 \nmid v_K(c)$ かつ $p \nmid v_K(c)$ となるものが存在し、$\delta_\phi \equiv \Delta^{\frac{1}{2}}/v_H(c)c \mod U_H^{a(\chi)}$ が成り立つ。さらに次の *Ogg* の公式も成り立つ。

$$a(E/K) = v_K(\Delta) - 2v_K(c) + 2.$$

特に Δ が *minimal* であることと $v_K(c) = \frac{m+1}{2}$ は同値。ここで m は E/K^{un} の *Néron* モデルの *special fibre* の *component* の数である。また常に $v_K(c) \equiv \frac{m+1}{2} \mod 6$ が成り立ち、E のタイプはこの値で決定される。

Proof. 詳細は省略して key point だけ述べる。まずこのような Weierstraß 方程式は Tate algorithm (例えば Silverman [10]) の課程で得られる。次に δ_ϕ の計算。$a(M/H)$ を M/H の導手としよう。導手の定義から $g\pi_M/\pi_M = 1 + \pi_M^{a(M/H)-1}u$ を満たす単数 u が存在する。この式の両辺を $v_M(\alpha)$ 乗すると $v_M(\alpha)(1 - g\pi_M/\pi_M) \equiv 1 - g\alpha/\alpha \mod \pi_M^{a(M/H)}$。この式のノルムをとればよい。Ogg の公式について。仮に $\sigma_E = \mathrm{ind}_{H/K}\chi$ と書けたとしよう。Theorem 3.1 より χ は $\mathrm{Gal}(L/H)$ の忠実な指標と思える。よって χ の導手は M/H のそれと一致する。ゆえに Ogg の公式は誘導表現に対する導手公式 (c.f. Serre [9]) からの帰結である。σ_E が指標の直和になるときも同様である。最後の主張は $v_K(\Delta)$ は modulo 12 で一意的であることと普通の Ogg の公式 $a(E/K) = v_K(\Delta_{\min}) - m + 1$ から従う。 □

以下 Proposition 3.6 を使って $w(E/K)$ を計算していくのだが、tame の場合と違って易しくはない。その原因は $\chi(\delta_\phi)$、G_H が ϕ の取り方に依存することである。一方それらの積で表わされる $w(E/K)$ は ϕ に依存しないから、2 つの値を結ぶ関係式をみつけるのが問題となる。これから我々は $\chi(\delta_\phi)$ もガウス和 G_H を使って表わせることをみる。

$\mathcal{E}_L$ を E/L の Néron モデルとしよう。このとき任意の $g \in W_K$ に対し、$\mathcal{E}_L$ の automorphism で次のダイアグラムを可換にするものが一意に存在する (Néron モデルの universality)。それをまた g と書こう。

$$\begin{array}{ccc} \mathcal{E}_L & \xrightarrow{g} & \mathcal{E}_L \\ \downarrow & & \downarrow \\ \mathrm{Spec}\, O_L & \xrightarrow{g} & \mathrm{Spec}\, O_L. \end{array}$$

Proposition 3.8. $p=3$、σ_E は *wild* としよう。N を $K(\Delta^{\frac{1}{4}})$ の有限次拡大で、E はそこ上 *good reduction* をもつとする。また $\Phi_N \in W_N$ を $\mathrm{Gal}(\overline{k}/k_N)$ の ' 幾何学的 ' フロベニウスのもち上げとする。このとき $\mathcal{E}_L$ の *automorphism* として

$$\Phi_N = -\sum_{u\in k_N^\times}\left(\frac{u}{k_N}\right) g_\phi^{\mathrm{Tr}_{k_N/\mathbb{F}_3(u)}}.$$

証明は後に回し、まずはその系から。これが $\chi(\delta_\phi)$ を G_H で表わす関係式を与える。

Corollary 3.9. $\Phi_N \in W_N$ を $\mathrm{Gal}(\overline{k}/k_N)$ の ' 算術的 ' フロベニウスのもち上げとする。このとき *Tate module* $V_l(E)$ への *action* として、

$$\Phi_N = -\sum_{u\in k_N^\times}\left(\frac{u}{k_N}\right) g_\phi^{-\mathrm{Tr}_{k_N/\mathbb{F}_3(u)}}.$$

Proof. $\mathcal{E}_L$ の generic fibre は $E\otimes_K L$ で K 上定義されている。これより $g\in W_K$ は generic には $1\otimes g$ で作用する。つまり $g\in \mathrm{Aut}(\mathcal{E}_L)$ は generic fibre の Tate module 上に自然なガロワ作用 g^{-1} を引き起こす。 □

この系を認めて既約かつ wild な σ_E に対する $w(E/K)$ の公式を証明しよう。

Proposition 3.10. *Proposition 3.6* と同じ仮定と記号のもとで

$$\chi(\delta_\phi)=\chi(-\Delta^{\frac{1}{2}}/v_H(c)c)\sim(\Delta\,,v_K(c)\,c)_v(-G_H)^{v_H(\Delta)/2}$$

Proof. 最初の等式は Proposition 3.7 よりわかる。まず $\chi(v_H(c)c)$ を計算しよう。Proposition 3.5 の証明の中にあるように $\chi|_{K^\times}=\eta\cdot\|\ \|_K$。一方 η は Hilbert 記号の定義から $x\mapsto(\Delta,x)_v$。よって $\chi(v_H(c)c)\sim(\Delta\,,v_H(c)\,c)_v=\left(\frac{-1}{k}\right)^{v_K(\Delta)}(\Delta\,,v_K(c)\,c)_v$。

次に $\chi(-\Delta^{\frac{1}{2}})=\left(-\left(\frac{-1}{k_H}\right)G_H\right)^{v_H(\Delta)/2}$ を示そう。Corollary 3.9 を $N=K(E[2],\Delta^{\frac{1}{4}})$ に適用する。今簡単のため $v_K(\Delta)$ は 4 の倍数でないとしよう。したがって $k_N=k_H$ である。これより W_H の算術的フロベニウス Φ で、$E[2]$ と $\Delta^{\frac{1}{4}}$ を固定するものがとれる。Φ_N として Φ をとれば $\chi(\Phi^{v_H(\Delta)/2})=\left(-\left(\frac{-1}{k_H}\right)G_H\right)^{v_H(\Delta)/2}$。ゆえに $\Psi\in W_H$ を相互写像で $-\Delta^{\frac{1}{2}}$ に対応するものとしたとき、$\chi(\Psi)=\chi(\Phi^{v_H(\Delta)/2})$ を示せば十分である。つまり $\Psi\circ\Phi^{-v_H(\Delta)/2}$ が L の元を固定することをみればよい。K^{un} を固定することは付値が 0 であることから従う。あとは Ψ が N を固定することをみればよいが、それは $-\Delta^{\frac{1}{2}}$ が N からのノルムになっていることからわかる。実際 $-\Delta^{\frac{1}{2}}=N_{N/H}\sqrt{\alpha-\beta}$。 □

$w(E/K)$ の公式は Proposition 3.6 と 3.10 を合わせて得られる。実際、$w(E/K)=\pm1$ は一般論によって知れれているので (c.f. Rohrich [7]) 1 の 3 巾乗根は符号に寄与しない。ガウス和は偶数巾になっていることがわかるので、符合はよく知られている。(Hasse-Davenport の定理を使って計算できる。)

Proposition 3.8 の証明の概略を述べよう。$\mathcal{E}_K$ を E/K の Néron モデルとし $\mathcal{E}_K\otimes O_L$ と $\mathcal{E}_L$ の generic fibre 間の同型を固定する。このとき Néron モデルの universality より $\iota:\mathcal{E}_K\otimes L\to\mathcal{E}_L$ over O_L が一意に存在し、次のダイアグラムが可換になる。

$$\begin{array}{ccc}\mathcal{E}_K\otimes O_L & \xrightarrow{\iota} & \mathcal{E}_L\\ {\scriptstyle 1\otimes g}\downarrow & & \downarrow{\scriptstyle g}\\ \mathcal{E}_K\otimes O_L & \xrightarrow[\iota]{} & \mathcal{E}_L.\end{array}$$

従ってもし ι がわかれば 上のダイアグラムを半時計回りに見ることによって $g: \mathcal{E}_L \to \mathcal{E}_L$ がわかる。

$\mathcal{E}_L$ と ι を具体的に定めよう。

Proposition 3.11. $\mathcal{E}_L$ を $\mathbb{P}^3_{O_L}$ の *closed subscheme* で アファイン座標: $Y^2 = X(X+1)(X-\frac{\gamma-\alpha}{\alpha-\beta})$ で定義されるものとする。このとき $\mathcal{E}_L$ は E の *smooth proper* モデルで *special fibre* は $\widetilde{\mathcal{E}_L}: y^2 = x^3 - x$ で与えられる。

Proof. $\mathcal{E}_L$ の generic fibre E_L が $E \otimes L$ と 同型であることをみよう。まず $\alpha - \beta$ の平方根 $\sqrt{\alpha-\beta}$ を固定する。このとき同型は $x = (\alpha-\beta)X + \alpha, y = \sqrt{\alpha-\beta}^3 Y$ で与えられる。smoothness を保障する最後の主張は、$N_{M/H}(\frac{\beta-\gamma}{\alpha-\beta}) = 1$ より $\frac{\beta-\gamma}{\alpha-\beta}$ は reduction すると 1 であることからわかる。 □

ι として上の証明の同型から誘導されるものをとろう。Proposition 3.8 は reduction して示せば十分である。ゆえに次の 2 つの命題から従う。

Proposition 3.12. g_ϕ、Φ_N を *Proposition 3.8* と同じとする。このとき g_ϕ は $\widetilde{\mathcal{E}_L}: y^2 = x^3 - x$ の *automorphism* $x \mapsto x+1, y \mapsto y$ を引き起こす。Φ_N は $\sharp k_N$ 巾フロベニウスを引き起こす。

Proposition 3.13 (The Gauss sum of $\widetilde{\mathcal{E}_L}$). $\mathbb{F}_q$ を $\mathbb{F}_3$ の有限次拡大とする。ρ を $\widetilde{\mathcal{E}_L}$ の *automorphism:* $x \mapsto x+1, y \mapsto y$ また Fr_q を q 巾フロベニウスとする。このとき

$$\mathrm{Fr}_q = -\sum_{u \in \mathbb{F}_q^\times} \left(\frac{u}{\mathbb{F}_q}\right) \rho^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3}(u)}.$$

証明は 2 つとも単純計算である。

4. 応用と計算例

ルートナンバー公式を使って Mordell-Weil 群の rank の偶奇を調べよう。もちろんまだ $p=2$ の場合の公式が知られていないので、ある種の条件を課さなければならない。例えば $p=2$ で potential mulitiplicative、tame、2 次拡大すれば good reduction になる場合などは 局所ルートナンバーを決定できる。また無限素点におけるルートナンバーは常に -1 である。(c.f. Rohrlich [7])

Example 1 $\quad y^2 = x^3 + D$ /$\mathbb{Q}$

この楕円曲線に対しては Liverance [6] による結果がある。彼の方法は CM 楕円曲線であることから Hecke character を詳しくしらべ、sextic reciplocity law を使う複雑なものである。しかしこれは我々の公式を使えば単純計算である。この場合 $p=2$ での局所ルートナンバーは $\pm(-1, D)_2$ である。$\pm$ は tame、wild に応じて 1 または -1。tame になるのは $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{-3})$ のときである。紙面の制約上 公式は次の特別な場合を述べるだけにとどめる。

Proposition 4.1. D を mod 4 で 1 となる整数で、*six power free* とする。また簡単のため $3 \nmid v_3(D)$ も仮定する。
$D = \pm 3^n {p_1}^{n_1} \cdots {p_k}^{n_k}$ と書くとき，$\mu(D)$ を $\mu(D) = \pm v_3(D) p_1 \cdots p_k$ で定義する。
このとき $E: y^2 = 4x^3 + D$ のルートナンバーは $w = -\left(\frac{\mu(D)}{3}\right)$ で与えられる。

Proof. $D \equiv 1 \mod 4$ という条件から E の minimal discriminant は $-3^3 D^2$ である。各素数 p に対し局所ルートナンバー w_p を決定する。$p \neq 3$、$p \mid D$ のとき、$3 \mid v_p(D)$

ならば E は p で I_0 タイプ、そうでなければ wild。これから $w_p = \left(\frac{p}{3}\right)(3,D)_p$ がわかる。$p=3$ のときは wild で、公式がよりただちに $w_3 = \left(\frac{v_3(D)}{3}\right)(3,D)_3$。無限遠点では $w_\infty = -1$ である。w_p をすべて掛け合わせて Hilbert の積公式を使えばよい。 □

Remark 4.1. $3 \mid v_3(D)$ の場合は $D = 3^{v_3(D)}D'$ と書き、座標変換 $x \leftrightarrow x - 3^{v_3(D)/3}D'$ を行う。そうすれば局所ルートナンバー公式が使える形になり、同様に計算できる。

Example 2

我々の公式は任意の局所体で成り立つ。したがって今度は楕円曲線を固定し、体を動かしてルートナンバーの変化を見るのも面白い。ルートナンバーが変化すればその体に新しく無限位数の有理点が登場したことになる。数体 F 上の楕円曲線 $E: y^2+y=x^3$ を例にとって見てみよう。判別式は $\Delta = -3^3$ なので悪い点は 3 の上のみである。

i) $K=\mathbb{Q}$ のとき、 $w=1$。
座標変換 $x \to x-1, y \to y+\frac{1}{2}$ すると $y^2 = x^3 - 3x^2 + 3x - \frac{3}{4}$。したがって E はタイプⅡである。公式より $w_3 = -(-27,-3)_3\left(\frac{-1}{3}\right) = -1$。無限遠点は 1 つだからルートナンバーは 1 となる。これから Mordell-Weil 群の rank は偶数であるが、Cremona の表によれば実際は 0 である。

ii) $K=\mathbb{Q}(\sqrt{d})$ のとき、$w = \mathrm{sign}(d)\left(\frac{d'}{3}\right)$。
d は square-free で $d = 3^a d'$、$a = 0, 1$ である。ここでは 2 通りの方法で計算してみよう。1 つは公式を直接計算する方法。もう 1 つは twist を考えて $\mathbb{Q}$ 上の話にする方法。

まずはダイレクトに公式を計算してみよう。$3 \nmid d$ のとき、素点 3 の上には $\left(\frac{d}{3}\right)$ の値に応じて、2 つまたは 1 つの素点がある。2 つあれば両方の素点の局所ルートナンバーが打ち消しあって 3 からの寄与はない。1 つのときは $K=\mathbb{Q}(\sqrt{d})$ のときと同様に -1 であることがわかる。つまり 3 からの寄与は $\left(\frac{d}{3}\right)$ である。$3 \mid d$ のときは 3 は K で分岐する。このとき $\Delta^{\frac{1}{2}} \in K$ と $\left(\frac{-d'}{3}\right)$ は同値である。これから 3 からの寄与は $\left(\frac{d'}{3}\right)$ であることがわかる。無限遠点の個数は d が正か負で 2 または 1 だから、寄与は d の正負に応じて 1 または -1。以上を全部かけあわせるとルートナンバーは $\mathrm{sign}(d)\left(\frac{d'}{3}\right)$。

つぎに twist をみる方法で計算してみよう。E の d による twist を E^d と書く。このときよく知られているように $\mathrm{rank}\, E(\mathbb{Q}(\sqrt{d})) = \mathrm{rank}\, E(\mathbb{Q}) + \mathrm{rank}\, E^d(\mathbb{Q})$。これから E の K でのルートナンバーは E と E^d の $\mathbb{Q}$ 上のルートナンバーを掛け合わせたもの（になるはず）である。E^d は $y^2 = x^3 - 3dx^2 + 3d^2x - \frac{3}{4}d^3$ で与えられ、判別式は $-d^6 3^3$。$p \mid d$、$p \neq 2, 3$ ならば、2 次拡大して good reduction になることから E^d は I_0 タイプ。したがって局所ルートナンバーは、$w_p = (-1,d)_p$。$p=3$ ならば E^d は wild で 局所ルートナンバーは $w_3 = \left(\frac{d'}{3}\right)(-1,d)_3$。$p=2$ ならば $\sqrt{d}$ を添加して E^d は good reduction になるから σ_{E^d} は可約。従って Proposition 3.5 と同様に $w_2 = (-1,d)_2$ がわかる。これらを全部掛け合わせて Hilbert の積公式から求めるものを得る。

またこの議論を逆にみれば、twist のルートナンバー公式は Hilbert の積公式そのものともいえる。

iii) $K=\mathbb{Q}(\zeta_p)$ $p\neq 2,3$ のとき、$w=-(-1)^{\frac{p-1}{f}}$。
ここで f は $p^f\equiv 1 \mod p$ となる最小の正の整数。証明は i)、ii) とほぼ同じなので省略する。

さて $p=7$ を例にとって体の拡大 $\mathbb{Q}\subset\mathbb{Q}(\sqrt{p^*})\subset\mathbb{Q}(\zeta_p)$ (ただし $p^*=\left(\frac{-1}{p}\right)p$) におけるルートナンバーの変化をみよう。上の公式からただちに 1、−1、1 と変化することがわかるので $\operatorname{rank} E(\mathbb{Q}(\zeta_p))\geq 2$。同様に $E: y^2+y=x^3-1$ についても計算すると、ルートナンバーは −1、1、−1 と変化するので $\operatorname{rank} E(\mathbb{Q}(\zeta_p))\geq 3$ がわかる。

References

[1] P. Deligne, Les constantes des equations fonctionelles des fonctions L, Modular Functions of One Variable IV, Lect.Note in Math 349.
[2] A. Fröhlich and J. Queyrut, On the functional equation of the Artin L-function for characters of real representations, Invent Math. 20(1973), 125-138.
[3] G. Henniart, Galois ε-factors modulo roots of unity. Invent. Math. 78 (1984), no. 1, 117–126.
[4] S. Kobayashi, The local root number of elliptic curves with wild ramification, preprint, 2000.
[5] A. Kraus, Sur le defaut de semi-stabilite des courbes elliptiques à reduction additive. Manuscripta Math. 69 (1990), no. 4, 353–385.
[6] E. Liverance, A formula for the root number of a family of elliptic curves. J. Number Theory 51 (1995), no. 2, 288–305.
[7] D.E. Rohrlich, Elliptic curves and the Weil-Deligne group. Elliptic curves and related topics, 125–157, CRM Proc. Lecture Notes, 4, Amer. Math. Soc., Providence, RI, 1994.
[8] D.E. Rohrlich,Variation of root number in families of elliptic curves ,Compositio mathmatica 87:119-151,1993.
[9] J.-P. Serre, Corps Locaux, Hermann, Paris, 1962.
[10] J.H. Silverman, Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.
[11] J. Tate, Number Theoretic Background, Proceedings of Symposia in Pure Mathmatics Vol.33 (1979), part 2, pp.3-26.